

In the Claims:

1 1. [Original] A method for a sender to send an encrypted message to
2 an authorized recipient, the method having steps comprising:
3 creating an encrypted content message that may be decrypted using a
4 content decryption key that is unknown to the authorized recipient;
5 creating an encrypted authentication message that may be decrypted
6 using a recipient's key wherein the recipient's key is known to the authorized
7 recipient but unknown to others except perhaps known to the sender;
8 fixing the encrypted authentication message and the encrypted content
9 message onto a tangible medium and thereafter permitting the authorized
10 recipient to obtain the tangible medium;
11 if a valid reply has been received, wherein the valid reply is based upon
12 the decrypted authentication message, then allowing the authorized recipient to
13 obtain said content decryption key.

1 2. [Original] The method of claim 1 wherein the recipient's key is a
2 secret key that is shared between the sender and the recipient.

1 3. [Original] The method of claim 1 wherein the recipient's key is a
2 recipient's private key that is associated with a recipient's public key.

1 4. [Original] The method of claim 1 wherein said step of creating an
2 encrypted authentication message further comprises a step of sender
3 authentication encryption such that the authorized recipient may use a sender's
4 key for decryption of the authentication message thereby authenticating that the
5 sender was the source of the encrypted authentication message, such that the
6 sender's key is known to the authorized recipient, and such that the encrypted
7 authentication message may be decrypted with a decryption step employing said
8 recipient's key and with another decryption step employing said sender's key.

*PDNO. 10003895-1
Serial No. 09/691,783
Amendment B*

1 5. [Original] The method of claim 4 wherein the sender's key is a
2 secret key that is shared between the sender and the authorized recipient but
3 unknown to others.

1 6. [Original] The method of claim 4 wherein the sender's key is a
2 public key that is associated with a sender's private key.

1 7. [Original] The method of claim 1 wherein said step of creating an
2 encrypted content message further comprises a step of sender authentication
3 encryption such that the authorized recipient may use a sender's key for
4 decryption of the encrypted content message thereby authenticating that the
5 sender was the source of the encrypted content message, such that the
6 sender's key is known by the authorized recipient, and such that the encrypted
7 content message may be decrypted by a decryption method with a step
8 employing the recipient's key and with another step employing the sender's key.

1 8. [Original] The method of claim 7 wherein the sender's key is a
2 secret key that is shared between the sender and the authorized recipient but
3 unknown to others.

1 9. [Original] The method of claim 4 wherein the sender's key is a
2 public key that is associated with a sender's private key.

1 10. [Original] An article of manufacture for sending an encrypted
2 message from a sender who possesses a content decryption key to a recipient
3 who possesses a recipient's key, the article, comprising:

4 a tangible medium;
5 an encrypted content message fixed on said tangible medium, wherein
6 said encrypted content message may be decrypted using the content decryption
7 key;

8 an encrypted authentication message fixed on said tangible medium,
9 wherein said encrypted authentication message may be decrypted using the
10 recipient's key;

*PDNO. 10003895-1
Serial No. 09/691,783
Amendment B*

11 whereby after the article is delivered to the recipient the recipient may
12 use the recipient's key to decrypt said encrypted authentication message into a
13 decrypted authentication message, the recipient may use the decrypted
14 authentication message to send a valid reply to the sender confirming that the
15 recipient received said article and the sender may then allow the recipient to
16 obtain the content decryption key.

1 11. [Original] The article of claim 10 wherein the recipient's key is a
2 secret key that is shared between the sender and the recipient.

1 12. [Original] The article of claim 10 wherein the recipient's key is a
2 recipient's private key that is associated with a recipient's public key.

1 13. [Original] The article of claim 10 wherein said encrypted
2 authentication message is sender authentication encrypted such that said
3 encrypted authentication message may be decrypted by a decryption method
4 having a step employing the recipient's key and having another step employing a
5 sender's key such that the recipient may use the sender's key to authenticate
6 that the sender was the source of said tangible medium.

1 14. [Original] The article of claim 13 wherein the sender's key is a
2 secret key that is shared between the sender and the authorized recipient but
3 unknown to others.

1 15. [Original] The article of claim 13 wherein the sender's key is a
2 public key that is associated with a sender's private key.
3

1 16. [Original] The article of claim 10 wherein said encrypted content
2 message is sender authentication encrypted such that said encrypted content
3 message may be decrypted by a decryption method having a step employing the
4 recipient's key and having another step employing a sender's key such that the
5 recipient may use the sender's key to authenticate that the sender was the
6 source of said tangible medium.

*PDNO. 10003895-1
Serial No. 09/691,783
Amendment B*

1 17. [Original] The article of claim 16 wherein the sender's key is a
2 secret key that is shared between the sender and the authorized recipient but
3 unknown to others.

1 18. [Original] The article of claim 16 wherein the sender's key is a
2 public key that is associated with a sender's private key.

1 19. [Original] A method for an authorized recipient to receive an
2 encrypted message from a sender, the method having steps comprising:
3 receiving a tangible medium from the sender wherein the tangible medium
4 has fixed upon it an encrypted authentication message and an encrypted content
5 message;
6 using a recipient's key to decrypt the encrypted authentication message
7 into a decrypted authentication message, wherein the recipient's key is known
8 to the authorized recipient but unknown to others except perhaps known to the
9 sender;
10 creating a valid reply using the decrypted authentication message;
11 sending the valid reply to the sender;
12 if the recipient has received a content decryption key from the sender,
13 then using the content decryption key to decrypt the encrypted content
14 message.

1 20. [Previously Presented] The method of claim 1 further comprising
2 receiving the valid reply using the sender after permitting the authorized
3 recipient to obtain the tangible medium, and wherein the allowing is responsive
4 to the receiving.

1 21. [Previously Presented] The method of claim 20 wherein the valid
2 reply is generated by the recipient after the recipient obtains the tangible
3 medium.

*PDNO. 10003895-1
Serial No. 09/691,783
Amendment B*

1 22. [Previously Presented] The method of claim 1 wherein the
2 creatings, the fixing and the allowing comprise creations, fixing and allowing
3 using the sender.

1 23. [Previously Presented] The method of claim 1 wherein the fixing
2 comprises permanently fixing the encrypted authentication message and the
3 encrypted content message onto said tangible medium.

1 24. [Previously Presented] The article of claim 10 wherein the
2 encrypted content message and the encrypted authentication message are
3 permanently fixed onto said tangible medium.

1 25. [Previously Presented] The method of claim 19 wherein the
2 creating and the sending the valid reply comprise creating and sending using the
3 authorized recipient.

1 26. [Previously Presented] The method of claim 19 wherein the
2 receiving, the usings, the creating, and the sending comprise receiving, usings,
3 creating and sending using the authorized recipient.

1 27. [New] The method of claim 1 wherein the fixing comprises fixing
2 both the encrypted authentication message and the encrypted content message
3 onto the tangible medium comprising the same medium.

1 28. [New] The method of claim 27 wherein the same medium
2 comprises a single fixed tangible medium.

1 29. [New] The method of claim 28 wherein the single fixed tangible
2 medium comprises a compact disc.

1 30. [New] The method of claim 19 wherein the using the recipient's
2 key comprises using the recipient's key by the authorized recipient.

*PDNO. 10003895-1
Serial No. 09/691,783
Amendment B*

7

- 1 31. [New] The method of claim 19 wherein the creating the valid reply
- 2 comprises creating using the authorized recipient.

PDNO. 10003895-1
Serial No. 09/691,783
Amendment B